

BBS2WWW

泄漏文件和目录内容漏洞

October 30, 2000

Sinbad Technical Publications
Website: <http://sinbad.zhoubin.com>
© Copyright 2000, All Rights Reserved

1.简介

BBS2WWW 是上海交大计算机应用工作室(<http://cas.tsx.org/>)专为 **Firebird BBS** 开发的 **WWW** 界面,它使得用户不必 **telnet** 登录到 **BBS** 中就可以使用 **BBS** 的各项功能。

BBS2WWW 1.33 版本中 CGI 函数存在一个缺陷,如果提交的链接中某些变量包含 "../" 字符串,远程用户就可能获取任何文件(以 **Web Server** 身份)的内容,也可以浏览有访问权限的目录。

另外,如果用户修改变量试图查看不存在的文件,将会泄漏 **bbs** 系统在硬盘上的物理路径。

2.细节

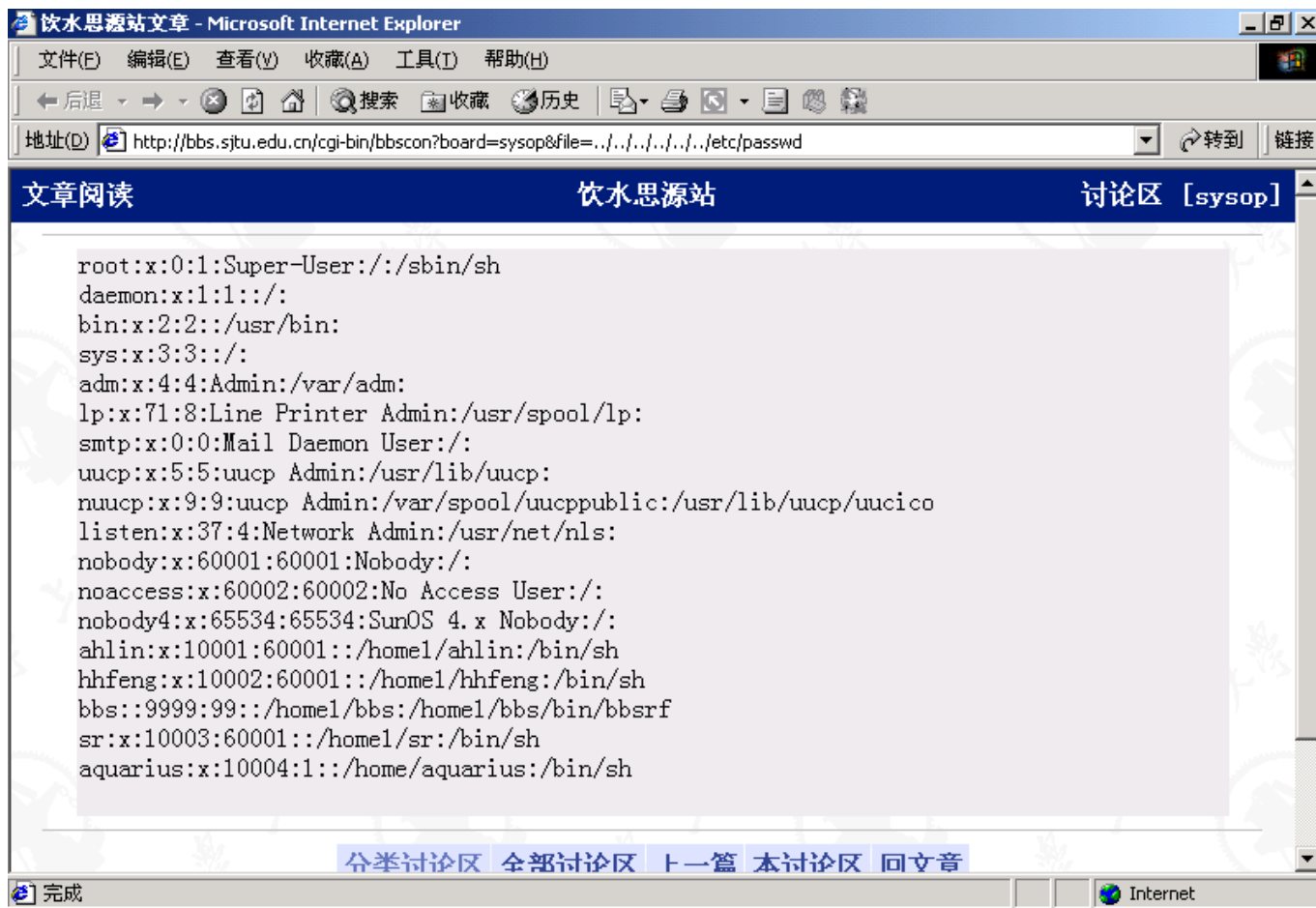
1. 泄漏 **BBS** 系统的物理路径

<http://bbs.sjtu.edu.cn/cgi-bin/bbscon?board=sysop&file=M.971439268>

将返回:

Error in opening file /home1/hhfeng/bbs/home/boards/sysop/M.971439268

2. 查看系统文件

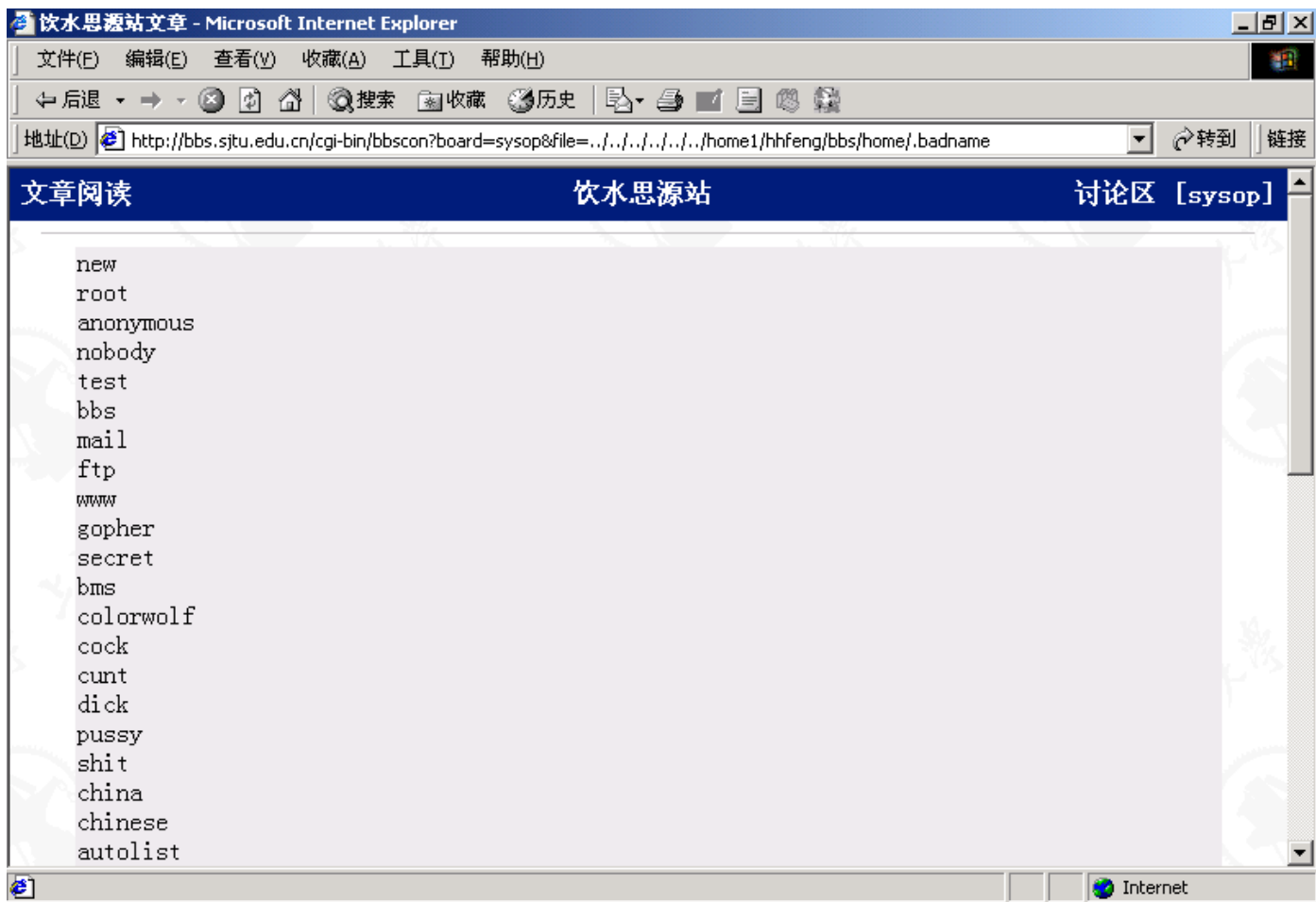


或者:

<http://bbs.victim.edu.cn/cgi-bin/bbscon?board=sysop&file=../../../../../../../../home1/hhfeng/g/bbs/home/.PASSWDS>

.PASSWDS 文件保存了 BBS 系统中用户的账号、密码等信息，如果被下载，可以用 John 进行暴力破解。

该 BBS 系统不允许注册的账号名如下图:



3. 解决方案

在拆分 Name/Value 对的 CGI 库函数部分，加上以下内容：

```
if (strstr (cgi_entries[i].value, "..") != NULL
    && strstr (cgi_entries[i].name, "passwd") == NULL
    && strstr (cgi_entries[i].name, "title") == NULL
    && strstr (cgi_entries[i].name, "text") == NULL )
show_error ("Error input!");
```

即除了用户密码、文章标题和文章内容，其它输入均需要过滤".."字符串。

国内很多高校 BBS2WWW 仍使用 1.33 或者以前的版本，请尽快修补或者升级。